INFRASTRUCTUREOUTSIDETHEPERIMETER · PART4OF4

The Clock You Do Not Set

Post-Quantum Cryptography and the Regulated Firm

David Newns, Substrate Advisory
July 2026

1. The structural fact

Every confidential connection a regulated firm makes, every certificate its systems trust and every digital-asset transaction its custody business signs rests on public-key cryptography: RSA and elliptic-curve cryptography foremost, whose security depends on problems no classical computer can solve in useful time. In 1994 Peter Shor published a quantum algorithm that solves those problems efficiently: a sufficiently capable quantum computer breaks the primitives outright. The replacement standards were published by the US National Institute of Standards and Technology in August 2024.[1] NIST's draft transition profile proposes deprecating the current algorithms after 2030 and disallowing them after 2035,[2] and on 22nd June 2026 Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, hardened those dates into binding federal deadlines.[3]

The thesis of this series is that each of four technologies, AI, cloud, public blockchain infrastructure and post-quantum cryptography, is driving changes in the regulatory environment, and that a licensed firm has three postures available: respond, exploit or ignore. For post-quantum cryptography the change arrived as a calendar rather than a perimeter: within eighteen months the G7 Cyber Expert Group published a coordinated financial-sector roadmap,[4] the EU set member-state milestones for 2026, 2030 and 2035,[5] the UK's National Cyber Security Centre set a three-stage national timeline running to 2035[6] and the US executive fixed 2030 and 2031 deadlines for its systems and contractors.[3] The reason this belongs on a board agenda this year rather than in 2029 is arithmetic: the first milestones fall within current planning horizons, hardware bought in 2026 will still be in service when the deadlines land, and the exposure on confidential data is governed by the date of capture, not the date any machine is built.

This report also differs from its predecessors in kind. Nothing here is closed or operated by others; the algorithms and the standards process are open to anyone. The gap is not auditability but control, timeline and sovereignty: the standards, the transition dates and the threat assessment behind them are set in the United States, and European firms are migrating on a clock they do not set.

2. The dependency as it stands

The cryptographic estate of a licensed firm decomposes into a small number of layers, and a board should be able to name its exposure at each. Transport encryption protects data moving between the firm, its clients and its counterparties. A public-key infrastructure of certificates establishes which systems and which pieces of software to trust, including the code-signing that guards releases into production. Hardware security modules, dedicated tamper-resistant devices that generate and guard cryptographic keys, anchor payments, custody and inter-firm message signing. And for a digital-asset business, the signatures on the chain itself are part of the estate: Bitcoin and Ethereum secure their wallets with elliptic-curve signatures, the primitive that Shor's algorithm breaks.[7] Almost all of this runs today on RSA or elliptic-curve cryptography, and all of it therefore shares a single common-mode exposure.

That exposure resolves into three distinct problems, each on a different clock.

Harvested data. Encrypted traffic and stored ciphertext captured today enter the at-risk pool the moment a cryptographically relevant machine exists, whatever the firm has migrated to by then. The governing date is the date of capture. The evidential position should be stated precisely, because it will be tested in any serious governance discussion: that adversaries collect encrypted data at scale is documented in disclosed intelligence programmes and now stated as the operating premise of US federal policy in the text of Executive Order 14412;[3] that the motive is retroactive decryption rests on government threat assessments rather than on attributed operational evidence, and no retroactive decryption has occurred or can yet occur.

Both halves of that sentence matter. The harvest is fact and the decryption is forecast; the asymmetry is that by the time the forecast could be confirmed, the loss would be retrospective and unbounded. For a private-banking franchise whose confidentiality obligations have no statutory expiry, data captured in 2026 is a 2040 problem incurred today.

Digital-asset custody. The protocol-level migration of the public chains to post-quantum signatures will be led by their own developer communities, whose incentive is existential, and a custodian will largely inherit it. What a custodian cannot inherit is the exposure that precedes migration: any address whose public key is already visible on-chain can be attacked the day a sufficiently capable quantum computer exists, whatever post-quantum scheme the chains later migrate to.[7] That exposure is set by the custodian's own key-management and address-reuse practices, which makes it the one part of the chain problem that is entirely within the firm's control today. The third report in this series examined the settlement-layer dependency in full; this is its cryptographic residue.

The certificate and hardware estate. Internal certificates, code signing and the HSM fleet are the most plannable of the three exposures, because they turn over on procurement cycles. In my experience that cycle runs five to seven years for an HSM fleet, which produces a piece of arithmetic every board can follow: the next refresh of any HSM bought in 2026 falls on or after the 2030 deprecation date, so the current procurement cycle is the migration cycle whether the institution plans it or not.

On the state of the threat itself, the neutral reference is the German Federal Office for Information Security's standing study of quantum-computer development, updated annually and most recently in version 2.2 of August 2025, which tracks hardware and cryptanalytic algorithms together and whose recent editions record steady progress towards cryptanalytic relevance as major error-correction roadblocks were resolved.[8] Two developments frame the current picture, and they must be kept apart. The first is on paper: in May 2025 a Google Quantum AI researcher published an estimate that a 2048-bit RSA key could be factored in under a week by a machine with fewer than one million noisy physical qubits, a twenty-fold reduction on the same author's 2019 estimate of twenty million.[9] The second is in hardware: IBM's published roadmap targets a fault-tolerant machine of around 200 logical qubits, error-corrected qubits each built from many physical ones, for 2029, and a successor of around 2,000 logical qubits beyond that; IBM itself does not present either as cryptographically relevant.[10] A paper resource estimate is not a machine, and no machine within orders of magnitude of the requirement exists. What the paper trend shows is that the requirement is falling independently of hardware progress, which is why practitioners have shortened their own deadlines: Cloudflare, which operates one of the largest cryptographic deployments in the world, moved its target for full post-quantum security forward to 2029 in April 2026, citing the continued fall in published resource estimates.[11]

The substitutability point that runs through this series lands here in inverted form. The primitive is, in principle, the most substitutable dependency of the four: the replacement algorithms are published, free and implementable by anyone. Yet the migration is the least substitutable programme, because cryptography is not a system but a property of every system at once, and the timetable is set externally. A firm can choose its cloud posture and its chain posture. It cannot choose whether elliptic-curve cryptography is deprecated in 2030.

3. The regulatory response in motion

United States. NIST published the first three post-quantum standards, ML-KEM for key establishment and ML-DSA and SLH-DSA for signatures, on 13th August 2024.[1] Its transition profile, IR 8547, proposing deprecation of RSA-2048 and 256-bit elliptic-curve cryptography after 2030 and disallowance after 2035, remains formally in draft as at 18th July 2026, with the comment period closed since January 2025.[2] The draft status has ceased to matter in practice. Executive Order 14412 of 22nd June 2026 directs a government-wide migration: agencies must move high value assets and high impact systems to post-quantum key establishment by 31st December 2030 and to post-quantum digital signatures by 31st December 2031, name accountable migration officials, and the Federal Acquisition Regulation is to be amended so that covered federal contractors comply with the post-quantum FIPS standards.[3] The companion order of the same date, Executive Order 14413, commits the United States to delivering an advanced quantum computer at a Department of Energy facility and directs the harmonisation of export controls with like-minded countries to keep quantum-enabling technologies from countries of concern.[12] Read together, the two orders make the sovereignty point of this report concrete: the threat assessment that drives the global timetable sits inside the US executive, and the enabling technology joins advanced AI as a good controlled at the US border.

European Union. The Commission recommended a coordinated transition in April 2024, and the NIS Cooperation Group, the member-state cybersecurity body established under the NIS Directive, published the resulting Coordinated Implementation Roadmap on 23rd June 2025: national transition roadmaps and first pilots by the end of 2026, high-risk use cases migrated by the end of 2030 and the remainder, as far as practicable, by the end of 2035.[5] The dates track NIST's: every European roadmap published since 2024 anchors on transition dates set in the United States. Two features of the EU response matter for a licensed firm. First, it runs through the cybersecurity machinery, the NIS Cooperation Group, ENISA and national cyber authorities, not through financial supervision: as at July 2026, none of ESMA, the EBA, EIOPA or ECB Banking Supervision has published operational supervisory guidance on the transition for financial entities, and I am not aware of any equivalent from FINMA. Second, the absence of sectoral guidance does not suspend the obligation. DORA's ICT risk-management provisions, which have applied to financial entities since January 2025, require the identification and management of this class of risk in general terms,[13] and the firms that migrate ahead of specific guidance will set the evidence base that supervisors later codify.

United Kingdom. The NCSC published its migration timeline on 20th March 2025: discovery and planning to 2028, high-priority migration by 2031 and full migration by 2035.[6] The Bank of England's October 2025 approach paper treats quantum alongside AI and distributed-ledger technology,[14] and the FCA's October 2025 research note remains the most practical reference yet published by a financial supervisor.[15] The UK dates are advisory for most commercial organisations, but they define the technical baseline a supervisor or competent authority will reach for when it begins asking questions.

The financial sector internationally. The G7 Cyber Expert Group's roadmap of 13th January 2026 is the most senior financial-sector statement to date: it advises G7 finance ministries and central banks, encourages a coordinated migration through 2030 to 2035 and is explicit that it sets no guidance or regulatory expectations.[4] The BIS tested post-quantum cryptography in a TARGET2 setting in Project Leap, with Phase 2 published in December 2025,[16] and the Banco de España's 2024 occasional paper remains the most substantive central-bank treatment.[17] Closest to operational use is the work convened by Europol's Quantum Safe Financial Forum: its February 2025 call to action asked financial institutions and policymakers to prioritise the transition,[18] and its January 2026 report with FS-ISAC and the Canadian Forum for Digital Infrastructure Resilience supplies a prioritisation methodology that weighs the quantum

risk to a system, assessed on the shelf-life of its data, its exposure and the severity of compromise, against the time its migration will take.[19]

The pattern across jurisdictions is unlike anything in the first three reports. No perimeter is being extended, because there is nothing to license: the threat actor does not exist and the algorithms are public. What is being published, everywhere, is dates, and the dates converge on the 2030 to 2035 window. They are American dates, set by NIST's technical judgement and now enforced on the US federal estate and its contractors by executive order, and Europe has adopted them. A European board planning against 2030 is planning against a deadline whose driving estimate it cannot see and whose revision it would learn about from a press release.

4. What response looks like

The compliance floor for an EEA firm is DORA's general ICT risk-management obligation; there is, as yet, no PQC-specific supervisory requirement to comply with. That makes this the one topic in the series where nearly all of the distinguishing work sits above the floor, in five areas.

Build the cryptographic inventory first. Every roadmap in the previous section, from the NCSC's 2028 milestone to the EU's end-2026 milestone to EO 14412's agency directives, begins with the same step: an inventory of where public-key cryptography is used, in which protocols, protecting which data, with which dependencies. The Europol and FS-ISAC methodology is usable as published: for each system, establish the shelf-life of the data it protects and the migration time the system would need, and prioritise where long shelf-life meets long migration.[19] This is the board-tractable first step because it needs no new technology and no vendor or standards decision, and because every subsequent decision is blind without it. In my experience of operating regulated market infrastructure, the first pass is laborious and the refresh is close to mechanical, and the inventory changes the quality of every vendor negotiation that follows it.

Prioritise by data longevity, not system criticality. The harvest exposure inverts the usual operational-resilience triage. A payments system critical to today's operations but whose data is stale in a week ranks below an archive of client records whose confidentiality must hold for decades. For a private-banking or wealth franchise this ordering is uncomfortable and correct: the most exposed assets are the quiet ones.

Take the tractable half now. The migration divides into key establishment, which protects confidentiality and closes the harvest window, and signatures, which protect authenticity. The first is deployable today: hybrid schemes, which run a post-quantum and a classical algorithm together so that the connection remains secure unless both are broken, are supported in mainstream browsers and infrastructure, and by April 2026 more than 65 per cent of human traffic to Cloudflare's network was post-quantum encrypted.[11] A firm can close the harvest window on its external interfaces years before it touches a signature scheme, and the cost is a configuration programme, not a re-architecture. Signatures, certificates and the trust chains behind them are the long pole, which is why the hardware estate comes next.

Capture the HSM refresh cycle. Two dates make 2026 procurement decisive. The post-quantum algorithms are now approved for validation in FIPS 140-3 cryptographic modules, and on 21st September 2026 the older FIPS 140-2 certificates move to the historical list, ending their use for new US federal procurement.[20] Meanwhile EO 14412 directs NIST to accelerate module validation because certification throughput, not algorithm availability, is the bottleneck the US government itself identified.[3,21] The practical consequences for a firm buying or renewing HSMs, certificate authorities or key-management platforms this year: require validated support for the new standards or a contractually committed upgrade path to it,

require algorithm agility in firmware rather than fixed-function devices, and put the vendor's own migration roadmap into the contract. A device bought in 2026 without a post-quantum path will need replacing before it has depreciated.

Make agility the requirement, not the algorithm. Crypto-agility, the ability to change algorithms without re-engineering the systems around them, is the property that survives whatever happens to any individual standard. FIPS 203, 204 and 205 are a floor rather than a terminus, and the sensible contractual and architectural posture is to assume further algorithm churn through the 2030s. This is also where the custody business reconnects: a custodian cannot run the chains' protocol migration, but its own key-management, address-reuse and cold-storage practices determine how much of its estate is exposed in the interim, and an agility posture is what lets it follow the chains' migration quickly when it comes.[7]

The board metrics that fall out of this work are short: the share of the estate covered by the cryptographic inventory, the count of systems where data shelf-life extends past 2035 on quantum-vulnerable primitives, the proportion of external interfaces on hybrid post-quantum key establishment, and every HSM and certificate-authority refresh date plotted against 2030.

5. The advantage case

The advantage case here is real but should be stated at its actual weight, and it rests on a feature no other topic in this series has: the deadlines are fixed, public and external, so early is defined for the firm rather than by it.

The first advantage is cost, and it is the one with published evidence. The US federal government's own estimate for migrating its prioritised civilian systems is approximately 7.1 billion US dollars over 2025 to 2035, a figure OMB itself labels a rough order of magnitude with high uncertainty, and a large share of it is the replacement of systems that cannot accommodate new cryptography at all.[21] The cost structure of a late migration is the cost structure of that estimate's worst components: compressed timelines, scarce specialist capacity and forced replacement rather than scheduled refresh. A firm that captures its ordinary procurement cycles, as set out above, converts most of the migration into business-as-usual spend. The record of the one large early mover supports the mechanism: Cloudflare began its preparation in 2019 and had post-quantum key establishment enabled across its estate by 2022, two years before the final standards were published.[11]

The second advantage is positional. Counterparty due diligence and DORA sub-outsourcing chains are already carrying cryptographic questions downstream, and a firm that can answer from an inventory is an easier vendor and an easier client. When European financial supervisors do publish expectations, and the direction of the G7, EU and UK material makes that a matter of sequencing rather than doubt, the firms with inventories will absorb the guidance as a reporting exercise while the rest begin discovery under a deadline.

The honest caveats: I cannot evidence a funding-cost or valuation premium attaching to quantum readiness as at July 2026, and no European supervisor yet scores it. The claim that survives the evidence is narrower and still sufficient: against fixed dates, early is cheap and late is expensive, and the difference is documented at federal scale.

6. The cost of ignoring it

The documented record here is prospective by nature, and that should be said plainly: no loss from retroactive decryption has occurred anywhere, and none can until a cryptographically relevant machine exists. A board should not accept scare rhetoric on this topic, and it does not need to, because three documented facts do the work.

The first is the harvest. The collection of encrypted material at scale is the stated operating premise of current US federal policy, written into the operative text of EO 14412,[3] and the NCSC frames its own guidance around keeping today's confidential information secure in the years to come.[6] A firm that ignores the transition extends, daily, the pool of its own data sitting in the at-risk category, with the longest-lived confidentiality obligations accruing fastest.

The second is the calendar. Deprecation dates convert a technology position into a compliance position. From September 2026 the older module certifications lose validated status for new US federal use;[20] from the end of 2030 the US federal estate and its contractors must be off the vulnerable primitives for their most sensitive systems;[3] and the EU and UK milestones run on the same grid.[5,6] A European licensed firm is not directly bound by any of these instruments today. But its vendors sell into the jurisdictions that are, its counterparties assess against them, and the supervisory guidance that eventually arrives will be drafted against the same dates. The firm that has done nothing by 2030 will be explaining, to clients and in time to a supervisor, why its cryptographic estate stands where the US government was directed not to be.

The third is the migration time itself. The federal cost estimate and every published roadmap embed the same finding: the transition takes the better part of a decade even when begun deliberately, because it touches every system, depends on vendor and certification throughput outside the firm's control, and cannot be parallelised past a point.[4,21] Against fixed end-dates, time not used at the front of the window is capacity permanently lost from it.

7. Board questions

1. Do we hold a cryptographic inventory, what share of the estate does it cover, and can the executive show, for each critical system, the data shelf-life and the estimated migration time on the Europol and FS-ISAC pattern?
2. Which of our data holdings carry confidentiality obligations beyond 2035, and which of them transit or rest today on quantum-vulnerable key establishment that an adversary could be capturing now?
3. What proportion of our external interfaces already runs hybrid post-quantum key establishment, and what is the plan and date for the remainder?
4. Which HSMs, certificate authorities and key-management platforms refresh before 2031, and does every current procurement require validated post-quantum support or a contractual upgrade path with algorithm agility?
5. For our digital-asset custody activity, which holdings sit on signature schemes the transition will deprecate, and what do our address-reuse and key-exposure practices add to that exposure today?
6. Who owns the migration programme at executive level, against which external date is it planned, and what would we show a supervisor tomorrow if supervisory guidance landed on the published national timetables?

8. Sources and notes

1. NIST FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SLH-DSA), published 13th August 2024: https://csrc.nist.gov/pubs/fips/203/final ; https://csrc.nist.gov/pubs/fips/204/final ; https://csrc.nist.gov/pubs/fips/205/final
2. NIST IR 8547 (initial public draft, 12th November 2024; proposes deprecating current elliptic-curve cryptography and RSA-2048 after 2030 and disallowing them after 2035; comment period closed 10th January 2025; the document remains in draft as at 18th July 2026 and the dates are NIST's technical judgement): https://csrc.nist.gov/pubs/ir/8547/ipd
3. Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," signed 22nd June 2026, published 25th June 2026, 91 FR 38483, FR Doc 2026-12909 (harvest-now-decrypt-later premise in Section 1; migration of high value assets and high impact systems to post-quantum key establishment by 31st December 2030 and to post-quantum digital signatures by 31st December 2031; proposed Federal Acquisition Regulation rule requiring covered contractor compliance with post-quantum FIPS; direction to NIST to accelerate Cryptographic Module Validation Program validations): https://www.federalregister.gov/d/2026-12909 See also https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
4. G7 Cyber Expert Group, "Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector," 13th January 2026 (coordinated transition through 2030 to 2035; the statement is explicit that it sets no guidance or regulatory expectations). US Treasury: https://home.treasury.gov/news/press-releases/sb0355 Full text: https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf
5. NIS Cooperation Group, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," version 1.1 dated 11th June 2025, published 23rd June 2025, following Commission Recommendation (EU) 2024/1101 of 11th April 2024 (national transition roadmaps and pilots by 31st December 2026; high-risk use cases transitioned by 31st December 2030; remaining systems as far as practicable by 31st December 2035): https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
6. NCSC, "Timelines for migration to post-quantum cryptography," 20th March 2025 (discovery and planning to 2028; high-priority migration by 2031; full migration by 2035; framed around keeping today's confidential information secure in years to come): https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
7. Technical note: secp256k1 / ECDSA is the signing algorithm for Bitcoin and Ethereum; the curve is not a NIST-approved curve, but the same Shor's-algorithm vulnerability applies to all elliptic-curve cryptography of this family. On the custody exposure and the settlement-layer dependency more broadly, see the third report in this series, "The Settlement Layer Nobody Licenses."
8. BSI (German Federal Office for Information Security), "Status of quantum computer development / Entwicklungsstand Quantencomputer," annually updated study, version 2.2, August 2025 (the study team's announcement for the preceding edition records that major roadblocks on the mainstream fault-tolerant path were resolved in 2024): https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer.html
9. Gidney C, "How to factor 2048 bit RSA integers with less than a million noisy qubits," Google Quantum AI, arXiv:2505.15917, 21st May 2025 (paper resource estimate under stated physical assumptions, including a 0.1 per cent gate error rate and a surface-code cycle time of one microsecond; compares with the 20 million noisy qubits of Gidney and Ekerå 2019): https://arxiv.org/abs/2505.15917
10. IBM, "IBM Sets the Course to Build World's First Large-Scale, Fault-Tolerant Quantum Computer at New IBM Quantum Data Center," 10th June 2025 (IBM Quantum Starling targeted for 2029 with around 200 logical qubits and 100 million operations; successor system Blue Jay targeted at around 2,000 logical qubits; vendor roadmap targets rather than delivered capability, and not presented by IBM as cryptographically relevant): https://newsroom.ibm.com/2025-06-10-IBM-Sets-the-Course-to-Build-Worlds-First-Large-Scale,-Fault-Tolerant-Quantum-Computer-at-New-IBM-Quantum-Data-Center
11. Cloudflare, "Cloudflare targets 2029 for full post-quantum security," 7th April 2026 (over 65 per cent of human traffic to Cloudflare post-quantum encrypted; target for full post-quantum security, including authentication, brought forward to 2029 citing recent research; post-quantum encryption enabled for all websites and APIs in 2022, following preparation begun in 2019): https://blog.cloudflare.com/post-quantum-roadmap/
12. Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation," signed 22nd June 2026, published 25th June 2026, 91 FR 38487, FR Doc 2026-12910 (Quantum Computer for Application Development and Discovery Science initiative to deliver an advanced quantum computer at a Department of Energy facility; harmonisation of export controls with like-minded countries on quantum-enabling technologies):

https://www.govinfo.gov/content/pkg/FR-2026-06-25/pdf/2026-12910.pdf See also https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

13. Regulation (EU) 2022/2554 (Digital Operational Resilience Act), applying from 17th January 2025; Chapter II ICT risk-management framework and Article 28 register of information: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
14. Bank of England, "The Bank of England's approach to innovation in AI, DLT and quantum computing," 15th October 2025: https://www.bankofengland.co.uk/report/2025/the-boes-approach-to-innovation-in-ai-dlt-quantum-computing
15. FCA research note, "Quantum Computing Applications in Financial Services," 3rd October 2025 (Markham and Grassie): https://www.fca.org.uk/publications/research-notes/quantum-computing-applications-financial-services
16. BIS Project Leap Phase 2, BIS othp107, 11th December 2025 (post-quantum cryptography tested in a TARGET2 setting): https://www.bis.org/publ/othp107.htm
17. Banco de España, Documento Ocasional 2421, Noemí López Chamorro, 12th June 2024: https://doi.org/10.53479/36696
18. Europol, "Quantum Safe Financial Forum: a call to action," 7th February 2025: https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action
19. Europol, FS-ISAC and the Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience, "Prioritising Post-Quantum Cryptography Migration Activities in Financial Services," January 2026 (prioritisation methodology weighing quantum risk, driven by data shelf-life, against migration time; cryptographic inventory of public-key use cases as the first step): https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf
20. NIST, Cryptographic Module Validation Program (FIPS 140-2 validation certificates move to the historical list on 21st September 2026; FIPS 140-3 validations current, with ML-KEM, ML-DSA and SLH-DSA approved for validation in FIPS 140-3 modules): https://csrc.nist.gov/projects/cryptographic-module-validation-program
21. Office of Management and Budget, "Report on Post-Quantum Cryptography," report to Congress under the Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260), July 2024 (approximately 7.1 billion US dollars, in 2024 dollars, to migrate prioritised federal civilian information systems over 2025 to 2035; stated as a rough order of magnitude with high uncertainty; excludes national security systems; identifies replacement of systems that cannot accommodate new cryptography as a significant share of the estimate, and validation throughput as a constraint): https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

David Newns is an Advisor to BPX Markets Limited and an Independent Non-Executive Director of Axiology Group. The views expressed are personal and do not represent the positions of any organisation with which he is associated. Nothing in this report constitutes legal, regulatory or investment advice.